

CLAIMS

What is claimed is:

- 1 1. A method for network-based scanning for potentially malicious content,
2 comprising:
 - 3 (a) monitoring network communications over a network;
 - 4 (b) identifying potentially malicious content in the network communications;
 - 5 (c) quarantining the potentially malicious content of the network communications;
 - 6 (d) executing a pattern for testing the potentially malicious content network
7 communications for malicious code; and
 - 8 (e) conditionally delivering the network communications over the network based on
9 the testing.
- 1 2. The method as recited in claim 1, further comprising scanning the network
2 communications for known malicious content.
- 1 3. The method as recited in claim 1, wherein the malicious content includes a
2 mass-mailer virus.
- 1 4. The method as recited in claim 1, wherein content is identified as potentially
2 malicious when a number of instances of the content in the network
3 communications is greater than a predetermined value.
- 1 5. The method as recited in claim 1, wherein the network communications include
2 electronic mail messages.

1 6. The method as recited in claim 5, wherein an electronic mail message is
2 identified as having potentially malicious content when a number of messages
3 having an identical subject line is greater than a predetermined value.

1 7. The method as recited in claim 1, wherein the potentially malicious content is
2 quarantined until the potentially malicious content has been scanned with a
3 malicious code detection file received after the potentially malicious content.

1 8. The method as recited in claim 1, further comprising cleaning the potentially
2 malicious content if malicious code is found for disabling the malicious code.

1 9. A computer program product for network-based scanning for potentially
2 malicious content, comprising:
3 (a) computer code that monitors network communications over a network;
4 (b) computer code that identifies potentially malicious content in the network
5 communications;
6 (c) computer code that quarantines the potentially malicious content of the network
7 communications;
8 (d) computer code that executes a pattern for testing the potentially malicious
9 content network communications for malicious code; and
10 (e) computer code that conditionally delivers the network communications over the
11 network based on the testing.

1 10. A system for network-based scanning for potentially malicious content,
2 comprising:
3 (a) logic that monitors network communications over a network;
4 (b) logic that identifies potentially malicious content in the network
5 communications;

- 6 (c) logic that quarantines the potentially malicious content of the network
7 communications;
- 8 (d) logic that executes a pattern for testing the potentially malicious content network
9 communications for malicious code; and
- 10 (e) logic that conditionally delivers the network communications over the network
11 based on the testing.

1 11. A method for network-based scanning for potentially malicious content,
2 comprising:

- 3 (a) monitoring network communications over a network;
- 4 (b) identifying potentially malicious content in the network communications;
- 5 (c) quarantining the potentially malicious content of the network communications;
6 and
- 7 (d) delivering the network communications over the network after a predetermined
8 delay.

1 12. The method as recited in claim 11, further comprising scanning the network
2 communications for known malicious content.

1 13. The method as recited in claim 11, wherein content is identified as potentially
2 malicious when a number of instances of the content in the network
3 communications is greater than a predetermined value.

1 14. The method as recited in claim 11, wherein the network communications include
2 electronic mail messages.

1 15. The method as recited in claim 14, wherein an electronic mail message is
2 identified as having potentially malicious content when a number of messages
3 having an identical subject line is greater than a predetermined value.

1 16. The method as recited in claim 11, wherein the delay is for allowing
2 quarantining of the potentially malicious content until the potentially malicious
3 content has been scanned with a malicious code detection file received after the
4 potentially malicious content.

1 17. A method for network-based scanning for potentially malicious content,
2 comprising:
3 (a) monitoring network communications over a network;
4 (b) identifying potentially malicious content in the network communications;
5 (c) quarantining the potentially malicious content of the network communications;
6 and
7 (d) delivering the network communications over the network in response to a
8 request from a user.

1 18. The method as recited in claim 17, wherein the user is an intended recipient of
2 the quarantined network communications.

1 19. The method as recited in claim 17, further comprising scanning the network
2 communications for known malicious content.

1 20. The method as recited in claim 17, wherein content is identified as potentially
2 malicious when a number of instances of the content in the network
3 communications is greater than a predetermined value.

1 21. The method as recited in claim 17, wherein the network communications include
2 electronic mail messages.

1 22. The method as recited in claim 21, wherein an electronic mail message is
2 identified as having potentially malicious content when a number of messages
3 having an identical subject line is greater than a predetermined value.

1 23. A method for network-based scanning for potentially malicious content,
2 comprising:

3 (a) monitoring incoming and outgoing network communications over a network at a
4 gateway;

5 (b) scanning the network communications for known malicious content;

6 (c) identifying potentially malicious content in the network communications;

7 (d) wherein content is identified as potentially malicious when a number of identical
8 instances of the content in the network communications passing through the
9 network for a given period of time is greater than a predetermined value;

10 (e) wherein the network communications include electronic mail messages, wherein
11 an electronic mail message is identified as having potentially malicious content
12 when a number of messages having an identical subject line passing through the
13 network for a given period of time is greater than a predetermined value;

14 (f) quarantining the potentially malicious content of the network communications;

15 (g) delivering the network communications over the network upon occurrence of the
16 first of:

17 (i) scanning the potentially malicious content with a malicious code
18 detection file received after the potentially malicious content is
19 received;

20 (ii) upon receiving a user request;

21 (iii) upon passage of a predetermined amount of time;

- 22 (h) notifying an intended recipient of the potentially malicious content that the
- 23 potentially malicious content has been quarantined;
- 24 (i) notifying a sender of the potentially malicious content that the potentially
- 25 malicious content has been quarantined; and
- 26 (j) cleaning the potentially malicious content if malicious code is found for
- 27 disabling the malicious code.

1000549-13004
"SECRET"